УДК 323:351

Шинкаренко А.Ю.
Ставицький О.В.
канд. економ. наук, доцент
ORCID ID: 0000-0002-2114-0892
Національний технічний університет України
«Київський політехнічний інститут імені горя Сікорського»

КІБЕРБЕЗПЕКА ЯК ОДИН З МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОГО РОЗВИТКУ ЕКОНОМІКИ В УКРАЇНІ

КИБЕРБЕЗОПАСНОСТЬ КАК ОДИН ИЗ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ СТАБИЛЬНОГО РАЗВИТИЯ ЭКОНОМИКИ В УКРАИНЕ

CYBER SECURITY AS ONE OF THE MECHANISMS OF PROVIDING STABLE DEVELOPMENT OF ECONOMICS IN UKRAINE

У статті досліджено основні чинники, що впливають на ймовірність економічної структури стати жертвою кібератаки. Розглянуто і проаналізовано основні шляхи, інструменти і механізми реалізації кібератак. У статті проаналізовано причини і наслідки останніх наймасштабніших атак у кіберпросторі, які мали місце відбутися на території України і які були спрямовані, у тому числі, на стратегічно важливі для розвитку національної економіки структури. На основі проаналізованих даних, які були надані як українськими, так і закордонними компаніями, було визначено основні тенденції щодо розвитку механізмів і шляхів реалізації, зміни масштабів і частоти кібератак в залежності від розміру і рівня захисту економічної структури. У цій статті також проаналізовано основні механізми та інструменти захисту інформації. Визначено доцільність витрат спрямованих на захист інформації, стратегічно важливої для функціонування і розвитку будь-якої економічної структури.

Ключові слова: кібербезпека, інформаційна безпека, кібератака, збитки, системи захисту, інструменти захисту інформації, економічна структура.

В статье исследованы основные факторы, влияющие на вероятность экономической структуры стать жертвой кибератаки. Рассмотрены и проанализированы основные пути, инструменты и механизмы реализации кибератак. В статье проанализированы причины и последствия последних масштабных атак в киберпространстве, которые имели место состояться на территории Украины и были направлены, в том числе, на стратегически важные для развития национальной экономики структуры. На основе проанализированных данных, которые были предоставлены как украинскими, так и зарубежными компаниями, были определены основные тенденции развития механизмов и путей реализации, изменения масштабов и частоты кибератак в зависимости от размера и уровня защиты экономической структуры. В этой статье также проанализированы основные механизмы и инструменты защиты информации. Определена целесообразность расходов, направленных на защиту информации, стратегически важной для функционирования и развития любой экономической структуры.

Ключевые слова: кибербезопасность, информационная безопасность, кибератака, убытки, системы защиты, инструменты защиты информации, экономическая структура.

This article explores the main factors that affect the likelihood of becoming a victim of the economic structure cyber-attacks. Considered and analyzed basic ways, tools and mechanisms for implementing cyber-attacks. The article analyzes the causes and consequences of recent attacks in cyberspace largest, which were held in Ukraine and that, were sent, including the strategically important for the development of the national economy structure. Based on the analyzed data that were provided by Ukrainian and foreign companies, were the basic trends in the development of mechanisms and ways to implement changes the scale and frequency of cyber-attacks, depending on the size and level of protection of economic structure. This article also analyzes the main mechanisms and instruments of information security. Determined feasibility costs aimed at protecting the information strategically important for the functioning and development of any economic structure.

Keywords: cybersecurity, information security, cyberattack, losses, protection systems, information protection tools, economic structure.

Вступ. Із розвитком і запровадженням інформаційних технологій все гостріше постає питання кібербезпеки, а також традиційної інформаційної безпеки. Протягом останніх років значно зросла кількість і якість кібератак на різні сфери діяльності людини, зокрема на економічні структури. Заходи щодо забезпечення традиційної інформаційної безпеки і кібербезпеки призводять до витрат, а вдалі кібератаки – до збитків.

Актуальність даної теми очевидна, оскільки забезпечення безпеки роботи промислово стратегічних об’єктів є важливою складовою розвитку не лише окремо взятої структури, а і економіки країни в цілому.

Окрему увагу варто приділити авторам-науковцям, в працях яких розглядалася дана тематика дослідження, а саме: М. М. Безкоровайный, А. Л. Татузов, Д. В. Дубов,О. Шаховал, І. Лозова, С. Гнатюк, С. В. Мельник, О. А. Баранов, В. П. Харченко та ін.

Постановка завдання. Постає проблема розрахунку суми збитків внаслідок вдалих кібератак на економічну структуру.

Відповідно до поставленого завдання були поставлені такі цілі: визначити основні чинники, які зумовлюють, а також впливають на ймовірність кібератак; проаналізувати можливі наслідки, які можуть бути спричинені внаслідок успішних кібератак; з’ясувати ймовірні витрати на механізми безпеки інформації.

Методологія. При підготовці даного дослідження було використано методологію, що спирається на такі джерела інформації - університети, дослідницькі інститути, аналітичні центри і експертні опитування, дослідження статистичних і аналітичних агентств.

Для того, щоб дослідження мало більш глобальний характер були використані матеріали із академічних баз даних, електронних бібліотек, Інтернету, веб-сайтів спеціалізованих інституцій і інших джерел. Опрацювання цього набору даних і стало основою для визначення основних

тенденцій розвитку кібербезпеки і впливу кіберпростору на функціонування як окремих структур так і економіки в цілому.

Також були застосовані і загально наукові методи дослідження: аналізу, індукції, системного аналізу, абстрагування.

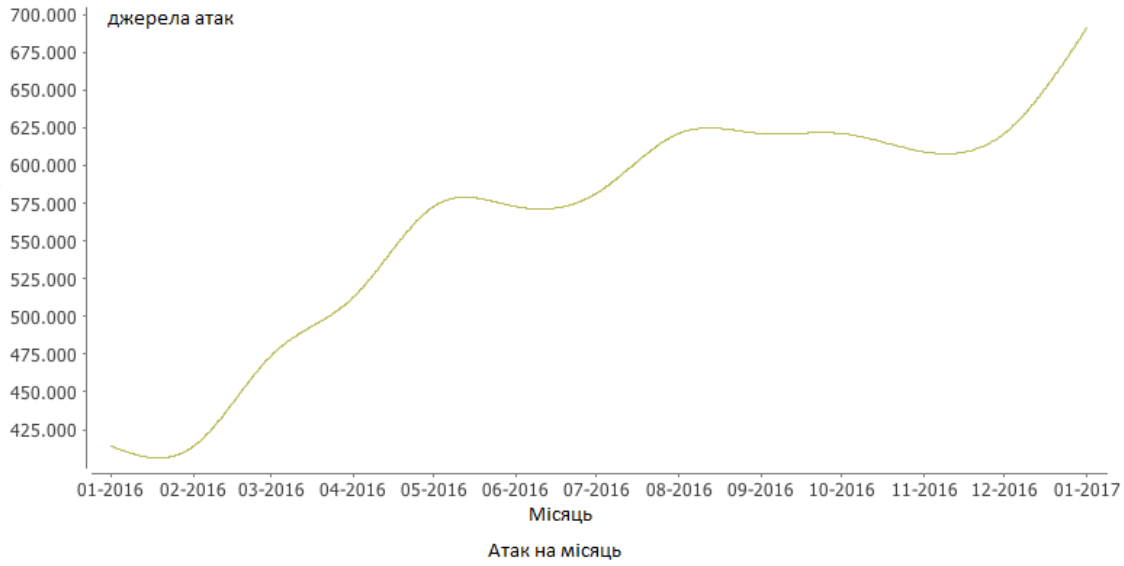
Результати дослідження. Відповідно до проаналізованих даних було встановлено основні закономірності щодо проведення кібератак на економічні структури:

– зростання складності структури атак, котрі можуть проводитись у декілька етапів, а також передбачувати більшість варіантів можливої протидії;

– вплив на веб-сервера, як носії і координатори стратегічно важливої інформації компанії;

– зростання частки кібератак як і на інформаційну інфраструктуру великих корпорацій, важливих промислових і стратегічних об’єктів, державних структур, так і на на малий і середній бізнес[1, с. 22].

На даний момент ми можемо відслідковувати тенденцію до зростання кількості джерел кібератак. Про це свідчать дані, що надає компанія Deutsche Telekom (графік 1)[5].



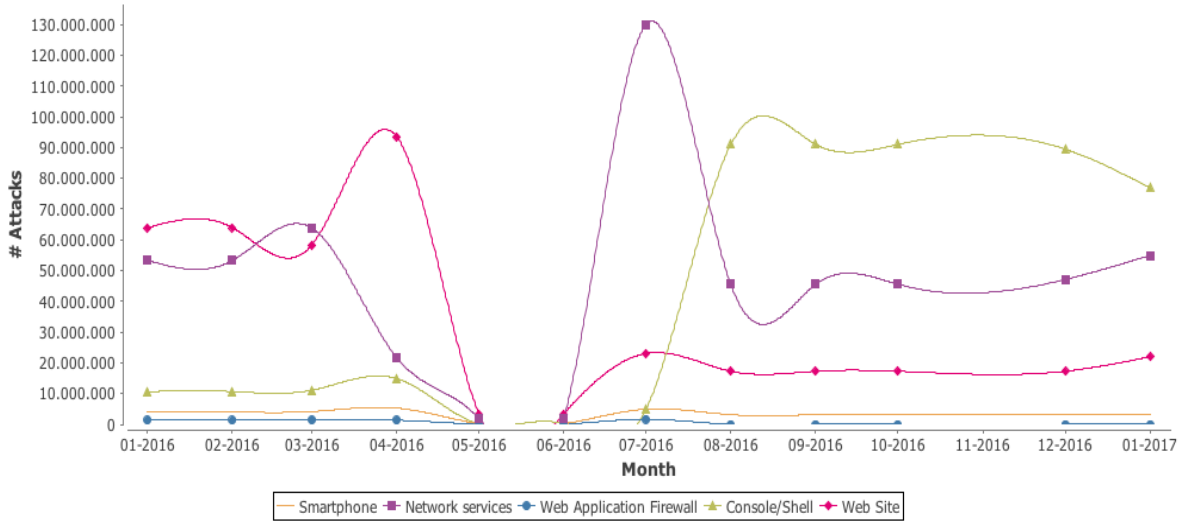
Графік 1. Кількість зафіксованих кібератак на місяць

Також можна прослідкувати тенденцію щодо вибору способу нападу на об’єкт. За останні п’ять місяців більшість кібератак були спрямовані на оболонку або консоль, тобто на частину операційної системи, що слугує інтерпретатором і на термінал системного адміністрування відповідно.

Про таку тенденцію при виборі механізму і спрямованості кібератаки свідчать статистичні дані надані Deutsche Telekom (графік 2) [5].

Успіх таких атак на пряму залежить від операційної системи машини на яку спрямована атака. Лідерами за кількістю встановлених систем

залишаються різні дистрибутиви Windows і Linux. Слід згадати, що обслуговування машини на Linux є дешевшим через безкоштовність цієї системи, проте також слід відзначити і відкритий код Linux, що допоможе атакуючій стороні виявити недоліки і слабкі місця у системі захисту. Взагалі дистрибутив операційної системи, який встановлений на обслуговуючій машині об’єкта є одним із визначних чинників, що впливають на рівень кіберзахищенності структури. Останнім часом популярними стали атаки на веб-сервера саме через ssh протокол, яий використовується для доступу до керування веб-сервера саме на системі Linux. Тобто такий вид кібератак – це фактично напад на сервер, на якому зберігаються стратегічно важливі дані, а також часто дані, котрі необхідні для координації веб-сайту або веб-сервісу об’єкта нападу. Особливою небезпекою таких атак є те, що вони майже повністю паралізують інформаційну інфраструктуру об’єкта нападу і збитки, спричинені, такою кібератакою, відповідно будуть глобальнішими.



Графік 2. Порівняння кількості кібератак на різні інформаційні структури на місяць

Характер і частота кібератак, а також масштаби збитків від них також залежить від сфери діяльності і масштабів структури об’єкта нападу.

Особливо негативні наслідки для виробничої сфери несуть за собою атаки на промислові об’єкти. Наслідками кібератак на промислові об'єкти можу бути не лише витік витоком конфіденційних даних і фінансові втратами, але і повна зупинка виробництва, що може призвести до техногенної катастрофи[2, с. 58]. Варто загадати кібератаку на інфраструктурні об’єкти України в галузі енергетики, котра відбулась 23 грудня 2015 року. Ця кібератака призвела до тимчасового масштабного відімкнення електроенергії як мінімум в трьох

регіонах України (на Прикарпатті, в Київській та Чернівецької областях). Загалом без електроенергії залишилось 220 тисяч споживачів (1% всіх енергокористувачів країни). А недовідпуск електроенергії становив 73 МВт-ч сумарною вартістю 79,5 тисяч гривень (0.015% від добового об'єму споживання України). А збитки на відновлення виробничого процесу і на налагодження інформаційної структури оцінюються приблизно 234,7 тис., грн. Проте ця сума не враховує тієї шкоди, яку може завдати підприємству атакуюча сторона, що під час проведення атаки отримала сратегічно важливу інформацію щодо технологічного процесу і фінансової звітності [6].

Кібератаки сильніше і частіше зачіпають малий і середній бізнес, оскільки такі компанії помилково вважають себе "нецікавими" в плані інформаційних ресурсів, котрими володіють.

Коли зломи стосуються великих організацій, то останні, як правило, потрапляють під приціл громадських ЗМІ. Однак насправді вони становлять лише невеликий відсоток від загальної кількості атак, які відбуваються щороку. На практиці, 71 відсоток зломів баз даних доводиться саме на малий бізнес.

Спрямований фішинг (Spear Phishing) і «Watering Holes» – найбільш поширені типи атак. У 91 відсотку кібератак фішинг є першою лінією атаки. У той час як традиційні фішинг-атаки розкинули широку мережу, розсилаючи електронні листи сотням або тисячам адресатів, спрямовані фішинг-атаки (гарпунний фішинг, Spear Phishing) націлені на невеликі підгрупи людей, як правило, співробітників компаній.

Шахрай, який планує спрямовану фішинг-атаку, може створити фальшивий електронну адресу співробітника і з нього написати кільком легітимним співробітникам, запитуючи інформацію про компанію. Думаючи, що вони спілкуються з колегою, легітимні співробітники можуть надати цю інформацію. І саме тут постає питання налаштування корпоративної пошти, а саме SPF цифрового підпису, значення якого і визначає сервера з яких можна надсилати пошту з корпоративного домену [4]. Також важливим етапом захисту є перевірка технічного заголовку листа, в якому міститься інформація про час надсилання листа і поштові сервери. Тож постає питання інструктажу робочого персоналу щодо основних правил інформаційної безпеки. Проведення такого тренінгу для робочого персоналу не призведе до великих затрат, проте може попередити досить значні загрози.

У разі використання стратегії атаки типу «Watering Holes» хакери розміщують шкідливі програми в коді веб-сайтів, які з найбільшою ймовірністю відвідують співробітники компанії, що атакується. Якщо працівник заходить на такий сайт з комп'ютера компанії, вся мережа компанії може піддатися вірусу, що збиратиме дані.

Причина того, чому кібератакам піддається саме малий і середній бізнес досить проста. Великі організації, як правило, зберігають важливі дані на власних серверах, в той час як малі та середні орендують віддалені сервера.

Малому та середньому бізнесу необхідно стати більш захищеними. За статистикою більше половини підприємств в Сполученому Королівстві не вживають будь-яких превентивних заходів, щоб захистити себе від кібератак. Крім того, 85 відсотків навіть не планують збільшити свої бюджети на безпеку, не дивлячись на той факт, що кількість атак зростає. Це робить малий і середній бізнес особливо привабливим для хакерів, які люблять легкі мішені.

Число шкідливих програм збільшується, і вони не розпізнаються. У минулому році, компанія Dell зібрала 37 мільйонів унікальних шкідливих зразків, що майже в два рази більше, ніж було зібрано в 2015 році. Коли ці атаки здійснюються опосередковано через «Watering Holes», немає меж, що визначають, що вірус буде поширюватися тільки на великі компанії. Тепер додамо той факт, що підприємства малого і середнього бізнесу мають менше захисних бар'єрів – закономірно, що малі підприємства відчувають максимальну вагу таких атак.

Малий і середній бізнес – ворота до великих корпорацій. В кінці 2013 року, хакери отримали номери кредитних карт 40 мільйонів клієнтів з бази даних пункту продажів Target, вкравши облікові дані у провайдера контактів Target – HVAC. Це був не тільки один з найбільших зломів в історії роздрібної торгівлі США, але він нагадав світу, як зловмисники можуть використовувати незахищених представників малого та середнього бізнесу в якості воріт до великих корпорацій [3]. Тобто до затрат на кібербезпеку можна додати не лише витрати на власні машини і обслуговуючі сервіси і механізми захисту, а також інвестиції у забезпечення кібербезпеки для малих компаній-партнерів, які володіють даними, що можуть бути використані для нападу на велику компанію.

Для більшості представників малого та середнього бізнесу зломи несуть важкі наслідки. Що робить цю тенденцію значним приводом для занепокоєння, так це те, що більша частина малого і середнього бізнесу просто не може пережити злом даних. Зломи можуть бути дорогими і, коли база даних не підлягає відновленню, організації малого і середнього бізнесу стикаються не тільки з репутаційними проблемами, але і з операційними – у 68 відсотків підприємств малого і середнього бізнесу немає тривалого бізнес-плану на випадок злому. Втрати виявляються настільки значними, що 60 відсотків змушені закритися протягом 6 місяців після злому даних.

Якщо додати до цих проблем високу поширеність втрати даних через загублених або вкрадених пристроїв, то стає очевидним, що для малого і середнього бізнесу настав час поставитися до питань безпеки даних більш серйозно.

Одна з найбільших переваг малого і середнього бізнесу – це здатність бути швидкими і мобільними. Команди таких підприємств іноді побоюються, що посилення безпеки означатиме втрату продуктивності, так як користувачі загрузнуть у процесах аутентифікації.

Однак є кілька способів для досягнення безпеки від хакерів і втрати або крадіжки девайсів без встановлення великої кількості обмежень на діяльність працівників, а також без вагомих фінансових затрат на забезпечення роботи такого механізму. Одним з прикладів таких способів захисту даних може виступати безперервне шифрування. Сьогодні можливо захистити дані, де б вони не зберігалися, – на мобільному чи пристрої або на настільному, в портативних чи медіа-сховищах або хмарі, – не ускладнюючи доступ для співробітників. З безперервним шифруванням, співробітники можуть мати доступ і обмінюватися даними, не витрачаючи час на надмірні заходи безпеки і не маючи справи з повільною завантаженням інформації.

Також інструментом захисту інформації може слугувати розширена аутентифікація, що об'єднує кілька форм аутентифікації для того, щоб переконатися в тому, що люди, які намагаються отримати доступ до даних компанії, є тими, ким вони представляються. Компанії можуть використовувати комбінацію апаратної аутентифікації, аутентифікації на основі облікового запису і шляхом цифрового підпису, щоб переконатися, що ніхто не отримає доступ до файлів, які їм не дозволено бачити.

Також не слід нехтувати програми стримування загроз. Сьогоднішні програми стримування шкідливих програм автоматично розпізнають і зупиняють шкідливі програми перш, ніж ті поширяться. Програми стримування загроз вказують браузерам запускати найбільш часті адресні програми у віртуальному середовищі. Таким чином, навіть якщо працівник відвідує сторінку, яка містить шкідливу програму, ця програма не може спрацювати і атакувати власника операційної системи. Крім того, ці системи можуть визначити шкідливі атаки, ґрунтуючись на поведінкових факторах, а не на підписах, тому компанія може зупинити поширення атак 0-day (zero-day загроза – zero-day; шкідливі програми, проти яких ще не розроблені захисні механізми).

Слід заначити, що більша частина вищезгаданих інструментів для захисту інформації є безкоштовними і водночас надійними. Тож робота кваліфікованого фахівця допоможе уникнути витрат на дороге програмне забезпечення.

Висновки. Таким чином, можна зробити висновок щодо основних чинників, що впливають на ймовірність для структури стати жертвою кібератаки. Відповідно визначено головні чинники: механізм захисту серверу, який зберігає, координує і передає важливі дані компанії; наявність цінної інформації у розпорядженні компанії; обізнаність працюючого персоналу з

питань інформаційної безпеки; використання інструментів розширеної аутентифікації, інструментів стримування поширення загроз тощо. Також слід зазначити, що втілення зазначених методів захисту інформації у роботі реальної економічної структури значно зменшить ризик стати жертвою кібератаки.

Література:

1. Безкоровайный М.М. Кибербезопасность подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. – 2014. – №1 (2). – С. 22-27. [Електронний ресурс] – Режим доступу: http://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya

2. Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України / О. Шаховал, І. Лозова, С. Гнатюк // Захист інформації. – том 18. – 2016. – №1. – 57-65. [Електронний ресурс] – Режим доступу:http://jrnl.nau.edu.ua/index.php/ZI/article/viewFile/10113/13301

3. Дубов Д.В. Стратегічні аспекти кібербезпеки України [Текст] / Дубов Дмитро Володимирович // Стратегічні пріоритети : [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. – Київ : НІСД, 2013. – 2013. № 4(29). – С. 119-126. – Бібліогр. : с. 125-126

4. http://www.openspf.org/SPF_Record_Syntax

5. http://www.sicherheitstacho.eu/

6.http://zillya.ua/zillya-antivirus-provela-analiz-kiberatak-na-infrastrukturni-ob-kti-ukra-ni